Robert C. Schubert S.B.N. 62684
Willem F. Jonckheer S.B.N. 178748
Amber L. Schubert S.B.N. 278696
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel.: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
wjonckheer@sjk.law
aschubert@sjk.law

Christian Levis (*pro hac vice* forthcoming)
Amanda Fiorilla (*pro hac vice* forthcoming)
Rachel Kesten (*pro hac vice* forthcoming)
Yuanchen Lu (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com
ylu@lowey.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

NICHOLAS RAPAK, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ADOBE INC.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Nicholas Rapak, individually and on behalf of all other similar situated individuals, asserts the following against Defendant Adobe Inc. ("Adobe") based upon personal knowledge, information and belief (where applicable), and the investigation of counsel.

SUMMARY OF ALLEGATIONS

1. The internet is not the Wild West. Individuals using the internet have a baseline expectation of privacy, in which they do not expect any company to engage in wide-spread surveillance of all their online activity, especially without affirmative consent.

2. Consistent with this expectation, several companies have begun to move away from user-based online tracking in recognition that it is privacy invasive. This began in the early 2010's, when Apple Inc. announced it would no longer allow companies to collect UDID, which is a permanent device identifier that was used for online advertising. Similar changes followed in the next decade, with the roll out of additional privacy-preserving features like Apple's "Do Not Track" setting, which sought to limit the collection of advertising IDs from mobile device users, as well as updates by several browsers to block "third-party" cookies (i.e., text files placed on a user's device from domains they are not visiting), which are used to track users across multiple websites.

3. Adobe did the opposite. While other companies moved away from privacy-invasive tracking technology, Adobe sought to capitalize on this shift by building a workaround that would track users regardless of browser, device, or settings. In addition to already-existing identifiers used by Adobe, it launched a new identity solution called the "Experience Cloud Identity Service" just after the deprecation of UDID, followed by the "Experience Platform Identity Service."

4. The **Experience Cloud Identity Service** filled the hole left by the removal of the UDID by Apple. Through this service, Adobe assigns a unique, persistent identifier—set via a first-party cookie—called the Experience Cloud ID ("ECID") to each website visitor. Companies using Adobe products—such as Adobe Analytics, Adobe Target**,** or Audience Manager—can deploy the ECID across their digital properties to uniquely identify individual users. Adobe also began assigning the "demdex.net" cookie to all its customers' unique users—which is closely tied to ECID—so it can track the same user across web properties owned by different organizations.

5. Building on ECID and the demdex.net cookie, Adobe then released **Adobe Experience Platform Identity Service**. Through this service, Adobe creates an "identity graph" that links "identities together." For instance, the identity graph will match the ECID to users' advertising identifiers (e.g., IDFA/ADID), and even more permanent forms of personally identifiable information, such as email addresses, phone numbers, usernames, and account numbers.

6. Adobe combines its Adobe Experience Platform Identity Service with other analytics and marketing products it offers, including **Adobe Real Time Customer Profiles**. These profiles merge multiple unique identifiers together, alongside data reflecting individual's private interactions and behaviors on the web properties. These profiles include user attributes (e.g., name, age, gender), behavior (e.g., private communications with website owners, such as user searches), audience membership (e.g., audiences the website owner has placed them in, such as "users who live in California"), and identifiers (e.g., email, phone, device identifiers, and cookies). This additional user data comes from Adobe's suite of marketing and analytics tracking technology found across the internet, including its Data Collection Tag. Using Adobe Real-Time Customer Profiles, Adobe can enrich the data and uncover even more information about the user, such as actions they are likely to take in the future.

7. Adobe's role as a centralized identity broker allows it to develop complete profiles of individuals and recognize them across websites and devices—exactly what privacy-preserving mechanisms are meant to prevent.

8. Adobe leverages the data collected through its Experience Cloud Identity Service—and the consumer profiles it creates—for its own benefit. For instance, Adobe allows customers to use these profiles in Adobe Target. Adobe charges customers to use Adobe Target, which leverages ECID and the Adobe consumer profiles, to create "personalized interactions" and "content" based on the individual's unique circumstances, such as where they live, what they are interested in, and what actions they have taken previously. Adobe also integrates its Experience Cloud Identity Service with its Audience Manager and Adobe Analytics, which are other ways companies can use these unique user profiles to target the individual user through Adobe.

9. Through these identity solutions—and complimentary products—Adobe has been secretly harvesting and monetizing directly identifiable user data from millions of U.S. residents without their knowledge and consent.

10. Plaintiff and Class Members had no knowledge that Adobe was using unique, persistent identifiers to track them and their private communications across the internet, or that it was using this data to facilitate targeted advertising.

11. Adobe itself does not disclose the extent of its persistent, user-specific tracking, nor does it prompt users viewing the websites or other web properties that use its identifiers of its presence, data collecting, or processes.

12. Adobe's interception of the contents of their communications with third parties through its tracking technology violates Cal. Penal Code § 631, and its installation of a tracking device on each of the websites they use across the internet violates Cal. Penal Code § 638.51(a), as well as other laws.

PARTIES

A. Plaintiff

13. Plaintiff Nicholas Rapak is a resident of Montgomery County, Pennsylvania.

14. Plaintiff Rapak used several online services, including Marriott's website, which implemented Adobe's identifiers and tracking software. Plaintiff Rapak visited and logged into Marriott's website via a web browser multiple times to search for and book Marriott hotels.

15. Unbeknownst to Plaintiff Rapak, Adobe assigned him an Adobe Experience Cloud ID (ECID) when he used certain online services, including Marriott's website.

16. Adobe also used other software to track Plaintiff Rapak, including Adobe Audience Manager, Adobe Analytics, and the Adobe Experience Platform script. Through this technology, Adobe intercepted, at least: (1) Plaintiff Rapak's searches on Marriott's website; and (2) full-string URLs revealing what Plaintiff Rapak was viewing and interacting with on Marriott's web properties. Adobe processed this data and stored it on its own servers for its own benefit and monetary gain.

17. Plaintiff Rapak did not consent to Adobe intercepting his unique identifiers and other personal data, assigning and using unique identifiers to track him across internet-enabled services and devices, or intercepting and using the contents of his private communications for-profit.

B. Defendant

18. Adobe is a Delaware corporation with its principal place of business located in San Jose, California.

19. Adobe knowingly and intentionally developed persistent, unique identifiers to track Plaintiff and Class Members across internet-connected services, despite knowing these types of identifiers were at odds with users' expectation of privacy.

20. Adobe knew that its identifiers, and especially Adobe Experience Cloud ID (ECID), circumvented existing privacy protections (like the deprecation of UDID) because it developed this identifier specifically as an alternative to such privacy-preserving mechanisms.

21. Adobe offered these services to websites, mobile applications, and other services so that it would have a unique way of tracking Plaintiff and Class Members across devices and platforms.

22. Adobe knowingly and intentionally used its identifiers, and data associated with it, to facilitate targeted advertisements for profit.

JURISDICTION AND VENUE

23. Jurisdiction is proper under 28 U.S.C § 1332(d) because: (1) the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, (2) there are more than 100 putative members of the Class, and (3) Plaintiff and a significant portion of Class Members are citizens of a state different from Adobe.

24. This Court has personal jurisdiction over Adobe because its principal place of business is in California. Additionally, this Court has personal jurisdiction over Adobe because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in California, including Adobe's interception and use of Plaintiff's unique identifiers and other personal data.

25. Venue is proper under 28 U.S.C. §1391(b), (c), and (d) because a substantial portion of the conduct described in this Class Action Complaint was carried out in this District. Furthermore, Adobe is headquartered in this District and subject to personal jurisdiction in this District.

26. This action arises in Santa Clara County, in that a substantial part of the events which gave rise to the claims asserted herein occurred in Santa Clara County. Pursuant to L.R. 3-2(e), all actions that arise in Santa Clara County shall be assigned to the San Jose Division.

BACKGROUND OF USER TRACKING

27. Over a decade ago, Apple announced it would no longer allow app developers to intercept "UDIDs" which are unique, device-specific identifiers. These persistent identifiers were deprecated because they are seen as privacy intrusive—they cannot be reset and were used to facilitate device-specific targeted advertising.

28. This trend only continued. Starting in 2020, Apple and Google announced the eventual deprecation of advertising identifiers (IDFA and ADID) and third-party cookies in favor of more privacy-preserving mechanisms.

29. The loss of some of the most common unique identifiers raised serious concerns within the multi-billion-dollar digital advertising industry. Digital advertisers relied on these identifiers and cookies to uniquely identify individuals who use their products and services—and other entities' products and services—to serve targeted advertisements to individuals, based on profiles of information reflecting web and app activity indexed to unique identifiers present in third-party cookies.

30. For instance, a mobile app developer would use identifiers like the IDFA and ADID created by iOS and Android phones to track user activity across their mobile application, understand what actions users took and their preferences, interests, and other information. The company would then send that information to an advertising company, such as Google, to serve targeted advertisements to that customer using this unique identifier.

31. Proposed solutions to make up for these unique identifiers and third-party cookies were not nearly as effective. For instance, some companies sought to track user "sessions" (i.e., one interaction with the webpage until the user closes out) in lieu of other unique identifiers. However, this alternative was not nearly as powerful as directly tracking an individual at the user or device-level.

ADOBE'S UNIQUE IDENTIFIERS

32. Adobe itself was well aware that there was a "rise in cookie regulation" as reflected in their own marketing materials.

FIGURE 1

33. Rather than embrace these changes, Adobe planned to capitalize on the move away from device identifiers and third-party cookies by Apple and Google by creating a persistent unique, cross-platform identifier of its own.

34. The first identity solution was called Adobe Analytics ID, which it now refers to as its legacy ID. This unique identifier is observable in network traffic as a cookie called s_vi. It is often stored as a first-party cookie and used to track a user across a single domain.

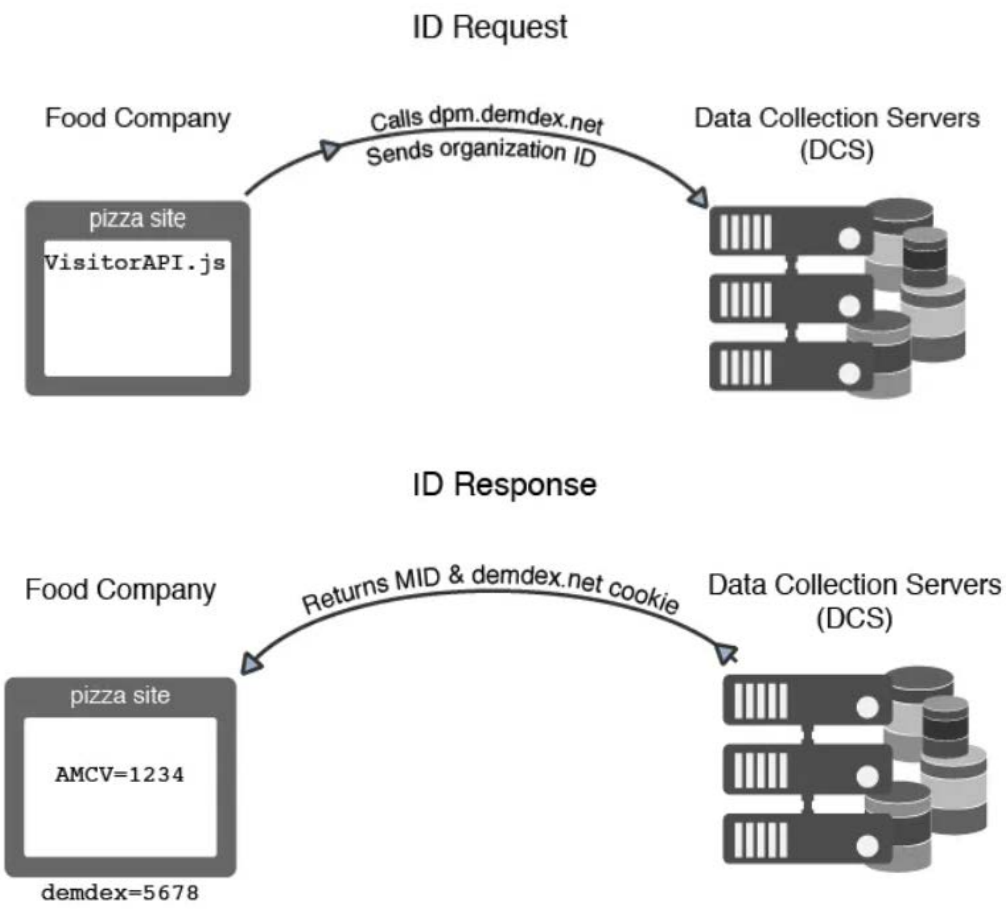
35. Adobe went on to develop **Adobe Experience Cloud Identity Service**, which introduced the Adobe Experience Cloud ID (ECID), also known as "MID." The ECID is a first-party cookie that assigns a persistent, unique identifier to each user and enables tracking across Adobe Experience Cloud products, including Analytics, Target, and Audience Manager. Through ECID, Adobe facilitates unified data collection and personalization consistently across their applications.

36. Thus, if a website domain owns two separate web properties, for instance, a hospital patient portal that uses Adobe Analytics and a public-facing website that uses Adobe Target, the same ECID will be assigned to the same user, even though they are different Adobe services. The ECID is stored in the field s_ecid and/or in an AMCV cookie. It can also be passed in parameters through network traffic. A single ECID cookie does not expire for two full years.

37. Adobe, however, also uses the ECID framework to track unique users across websites and online services owned by ***different*** companies. When a company initially sets the ECID, they call Adobe's "Data Collection Server" ("DCS") known as "dpm.demdex.net" and transmit their "organization ID."

Adobe's DCS processes this information and transmits back the user's ECID (identified in the Figure below as "MID") as well as a **demdex.net cookie**. This process is reflected in **Figure 2,** below.

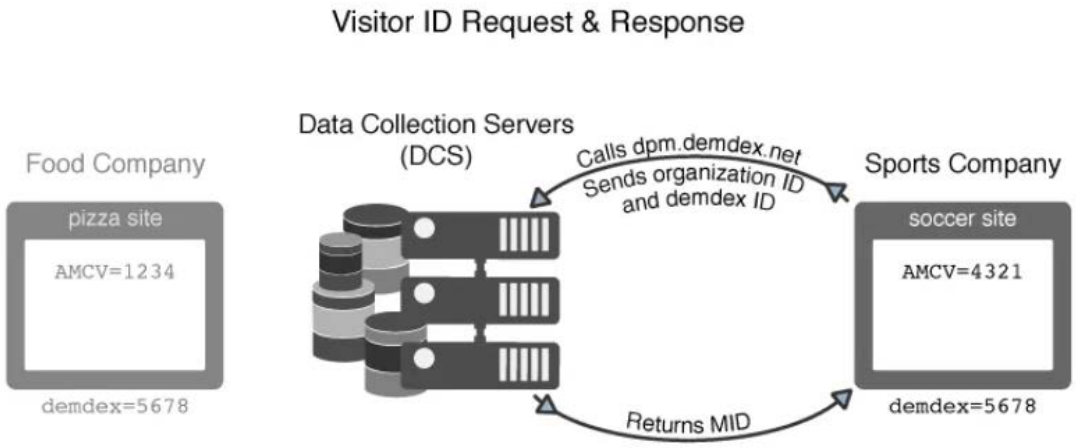
FIGURE 2[1]



38. In the above example, the demdex.net cookie set for the unique visitor who stopped at "Food Company" is 5678. Because the demdex.net cookie is persistent across websites—even those owned and operated by different website providers—when the "Food Company" user visits a new website, the demdex.net cookie continues to track them. This is reflected in **Figure 3**.

[1] *Identity Service Guide*, ADOBE, INC., https://experienceleague.adobe.com/en/docs/id-service/using/intro/id-request#concept-2caacebb1d244402816760e9b8bcef6a (last visited April 2, 2025).

FIGURE 3[2]



39. As shown in **Figure 3**, when the previous "Food Company" customer visits "Sports Company" Adobe's DCS assigns the same demdex.net cookie—5678. Thus, Adobe knows the same unique individual who visited "Food Company" is the same unique individual who visited "Sports Company."

40. If that were not enough, Adobe also assigned other unique identifiers. For instance, if there are "third-party cookie restrictions" Adobe sets a "fallback unique visitor ID" recognized as "s_fid" in network traffic, as well as "s.visitorID" which is another "unique identifier for the visitor." Adobe also collects IP address.

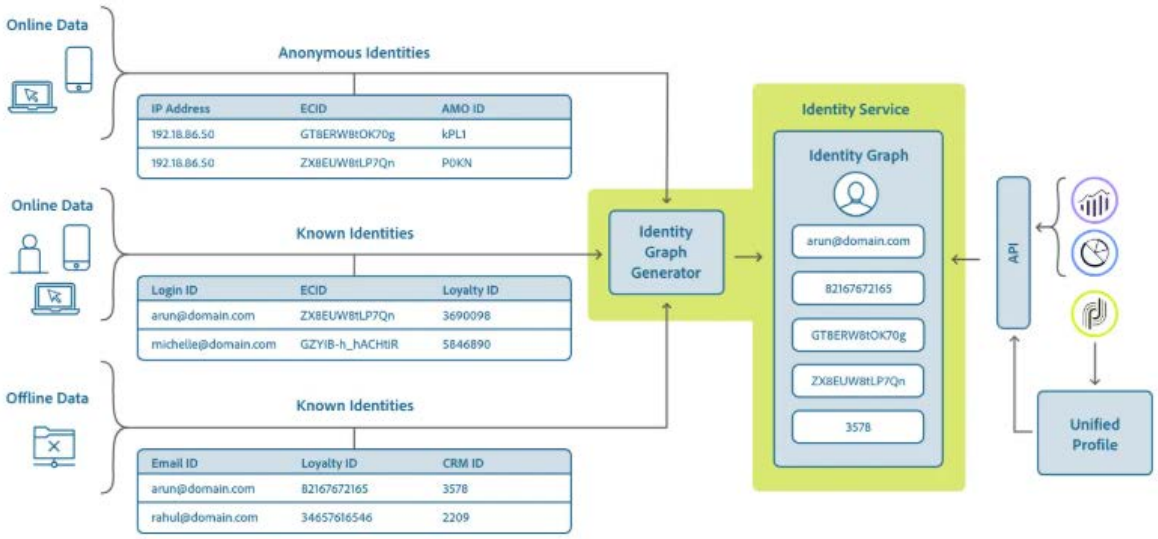
ADOBE'S COMPREHENSIVE IDENTITY SOLUTION

41. Adobe does not just provide identity solutions; it also launched the **Adobe Experience Platform Identity Service** to use these identifiers (and others) to profile users.

42. The Adobe Experience Platform Identity Service is designed to keep identity tracking consistent when the same user logs in or interacts with a website from multiple devices, such as from their phone and then their laptop, which would otherwise create multiple, disparate identifiers. Through this service, Adobe collects all the identifiers across devices and websites and links that to an "identity graph" through what it calls its "Identity Graph Generator." This associates all the known identifiers with the same individual, even though they would previously appear as multiple unique users.

[2] *Id.*

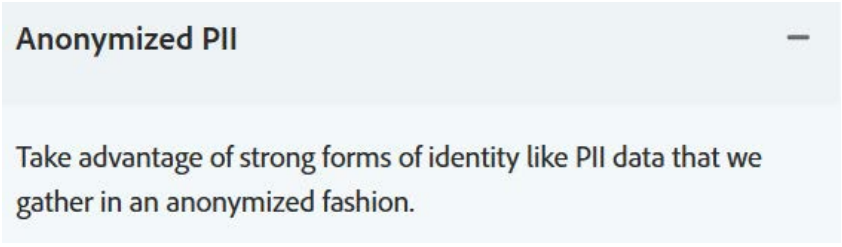
FIGURE 4[3]



43. As shown in **Figure 4**, through the Adobe Experience Platform Identity Service, Adobe receives identifiers, such as ECIDs, IP address, Login IDs, and email addresses, which it can then reconcile as the same user through its Identity Graph Generator.

44. Adobe incredibly bills its identity solution as gathering "PII data" in an "anonymized fashion." But both cannot be true at the same time. "Strong forms of identity" like PII data is exactly the opposite of anonymized data.

FIGURE 5[4]

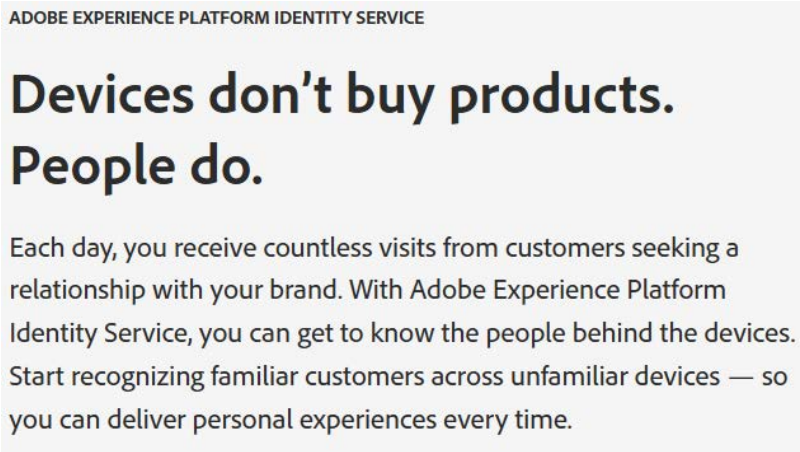


45. Despite its characterization, Adobe knew that this solution was ***better*** at tracking individuals than previous identifiers, including those being deprecated, and was not anonymized. Indeed, Adobe actively markets its identity solution as unique because it identifies the specific "***people behind the***

[3] *Platform Identity Service Guide*, ADOBE, INC., https://experienceleague.adobe.com/en/docs/experience-platform/identity/home (last visited April 2, 2025).
[4] *Experience Platform Identity Service*, ADOBE INC., https://business.adobe.com/products/experience-platform/identity-service.html (last visited Apr. 1, 2025).

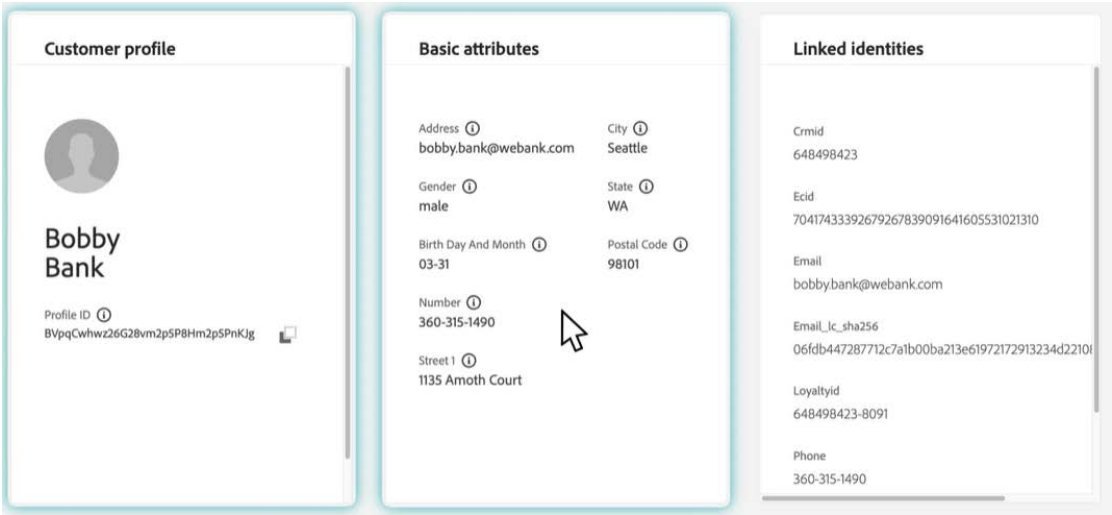
***devices*"**—not just devices.

FIGURE 6[5]



46. As shown in **Figure 6**, Adobe itself does not see its identity solutions as either a "session" or "device" level identifier, but a way to identify actual people, akin to a social media profile. **Figure 7** depicts what this profile looks like in the Adobe dashboard.

FIGURE 7



47. In fact, Adobe's identity solutions are ***stronger*** identifiers than those that previously existed, as Adobe itself acknowledges. For instance, most first-party cookies are limited in that they only track a user on one specific website. Adobe's Experience Platform Identity Service goes much further, by tracking users across permanent identifiers, such as email address and IP address, and first-party cookies like ECID. This makes it possible to create an identity profile that serves advertisers' needs, by aggregating

[5] *Id.*

data across all apps and websites a person uses that incorporates Adobe's technology, at the expense of individual's right to privacy.

48. Adobe's status as an identity broker allows it to track users across the internet and develop unique profiles, which Adobe then offers to its customers to use with Adobe's other marketing and analytics products at a price premium.

ADOBE'S EXPERIENCE CLOUD PLATFORM

49. Adobe created the Experience Platform Identity Service precisely because of its synergy with its existing (and pricey) analytics, advertising, and AI products. Collectively, all of these services are referred to as the **Adobe Experience Cloud Platform**. A subset of the services included in the Adobe Experience Cloud Platform are described below.

50. One of the products Adobe offers is **Adobe Analytics,** which includes its Data Collection Tag. This Adobe Data Collection Tag is deployed directly on web pages and mobile applications. When used, the Data Collection Tag automatically captures the ECID, along with other data and identifiers, including browser type, device characteristics, and IP address. It also collects more sensitive data revealing the user's communications with the website provider, including pages they visited, searches they conducted, and more. This information is transmitted directly to Adobe's own servers, as indicated by Adobe owned domains like demdex.net and adobedc.net.

51. The Adobe Data Collection Tag intercepts the Adobe Experience Cloud ID (ECID) and online users' private communications directly from webpages and redirects it to its own servers, aggregating that information with a user's profile, so it can be used for advertisements, including the creation of custom audiences, lookalike audiences, and campaign optimization.

52. The data collected through the Adobe Data Collection Tag is used for developing complex analytics, which reveal more information about the user than the data itself. For instance, Adobe offers **Predictive Analytics** (powered by Adobe Sensei), which it bills as "[p]redicting the future" i.e., future actions likely to be taken by the unique users whose data Adobe intercepted. As Adobe explains, "[h]idden in [the] data" are "patterns" that reveal additional "meaningful insights" that can be "used effectively" (through Adobe, of course) to have a "very real impact on the bottom line." Adobe provides predictive

analytics by running the intercepted data through "machine learning and advanced statistical models" to "dig automatically through [the] enormous amounts of data" and uncover new "insights" about the user.

53. **Adobe Audience Manager** is yet another product in the Adobe Experience Cloud Platform that works with Adobe Analytics and the Adobe Experience Platform Identity Service. In Adobe Audience Manager, Adobe customers can use its "proprietary algorithm" called "TraitWeight" to discover "new, unique audience members." The Adobe customer selects users and "trait[s]" or "segment[s]" associated with them—as identified through Adobe Analytics and the Adobe Experience Platform Identity Service—and then sends Adobe's algorithm to search the existing database for individuals likely to take similar actions as the originally selected individuals. Adobe's algorithm provides a "weighted score" reflected how similar the newly identifiers users are to the ones initially selected. Adobe Analytics can send data to Adobe Audience Manager in real-time through server-side forwarding.

54. **Adobe Campaign** similarly integrates with Adobe Analytics and the Adobe Experience Platform Identity Service. Adobe allows customers to use their "Analytics data directly in [Adobe] Campaign" with customer's other "email engagement data." Used together, Adobe customers can use audiences created in Adobe Analytics to send "personalized messages" based on "actions" they have taken on a website. Using "AI" Adobe Campaign can discern and "predict the best send times" that are the "most likely" to get customers to "engage."

55. Likewise, **Adobe Marketo Engage** also syncs with Adobe Analytics and the Adobe Experience Platform Identity Service. Adobe Marketo Engage tracks data like lead details, including users who completed forms, viewed certain pages, or engaged in email interactions. This data is synced through the Adobe Experience Platform Identity Service with data from Adobe Analytics in a unified profile. Adobe Analytics then enriches the Marketo Engage data to create lead scores and generate follow-up content to convert the lead to a customer or achieve some other marketing goal (i.e., converting to a paid customer, start trial, etc.).

56. **Adobe Journey Optimizer** is yet another product that can be integrated with Adobe Analytics and the Adobe Experience Platform Identity Service. Adobe Journey Optimizer allows customers to track user's interactions on a web property, and trigger certain responses based on the actions they take. For instance, if a user adds an item to cart, but does not purchase it, Adobe Journey Optimizer

flags this interaction and can be used to create the "perfect offer" to get the user to "engage" and "convert" by developing "targeted content." Adobe's AI can develop the targeted content directly for the Adobe customer.

57. Finally, **Adobe Advertising** also integrates with Adobe Analytics and the Adobe Experience Platform Identity Service. Combining Adobe Analytics with Adobe Advertising and Adobe Experience Platform Identity Service enables customers to perform remarketing, measure ad performance, and engage in campaign optimization based on unique user profiles compiled by Adobe. Adobe Advertising customers can use these profiles to buy, manage, and optimize advertisements directly through Adobe, which acts as a Demand-Side Platform for real-time bidding auctions. Adobe encourages customers to integrate Adobe Advertising with its other products precisely to provide this hyper-specific type of targeting and ad bidding.

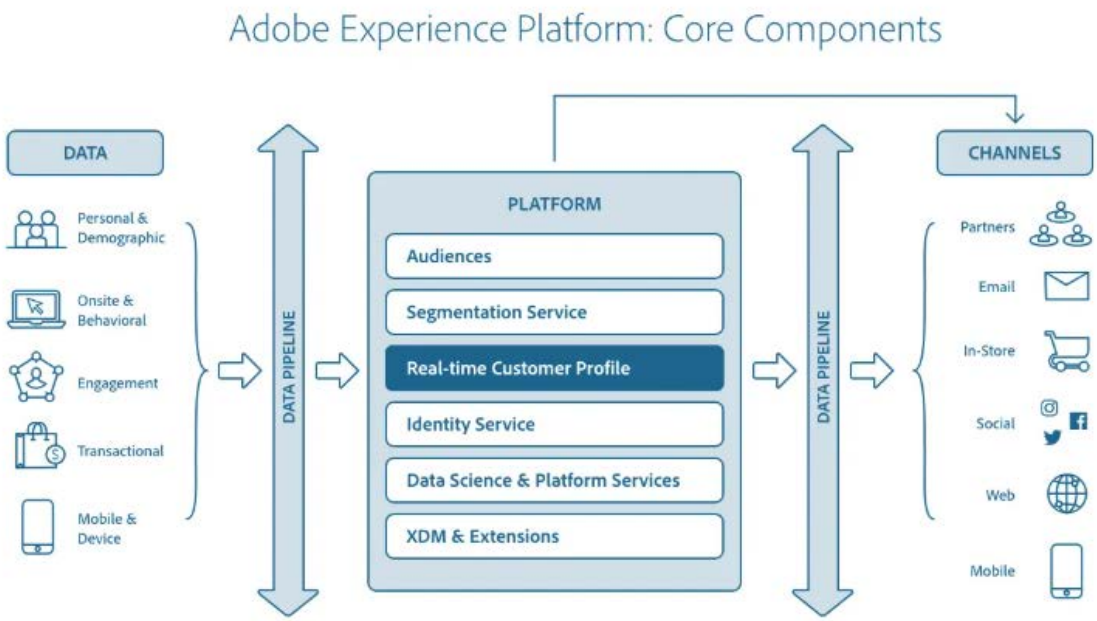
Adobe Product	**Integrates with Adobe Analytics**	**Integrates with Adobe Identity Solution**
Adobe Audience Manager	✓	✓
Adobe Campaign	✓	✓
Adobe Marketo Engage	✓	✓
Adobe Journey Optimizer	✓	✓
Adobe Advertising	✓	✓

ADOBE'S UNIQUE & COMPREHENSIVE USER PROFILES

58. Adobe offers a clear and easy way to combine the power of most of its marketing and analytics tools (including Adobe Analytics and Adobe Advertising) with the Adobe Experience Platform Identity Service all in one place. This is known as **Adobe Real-Time CDP**.

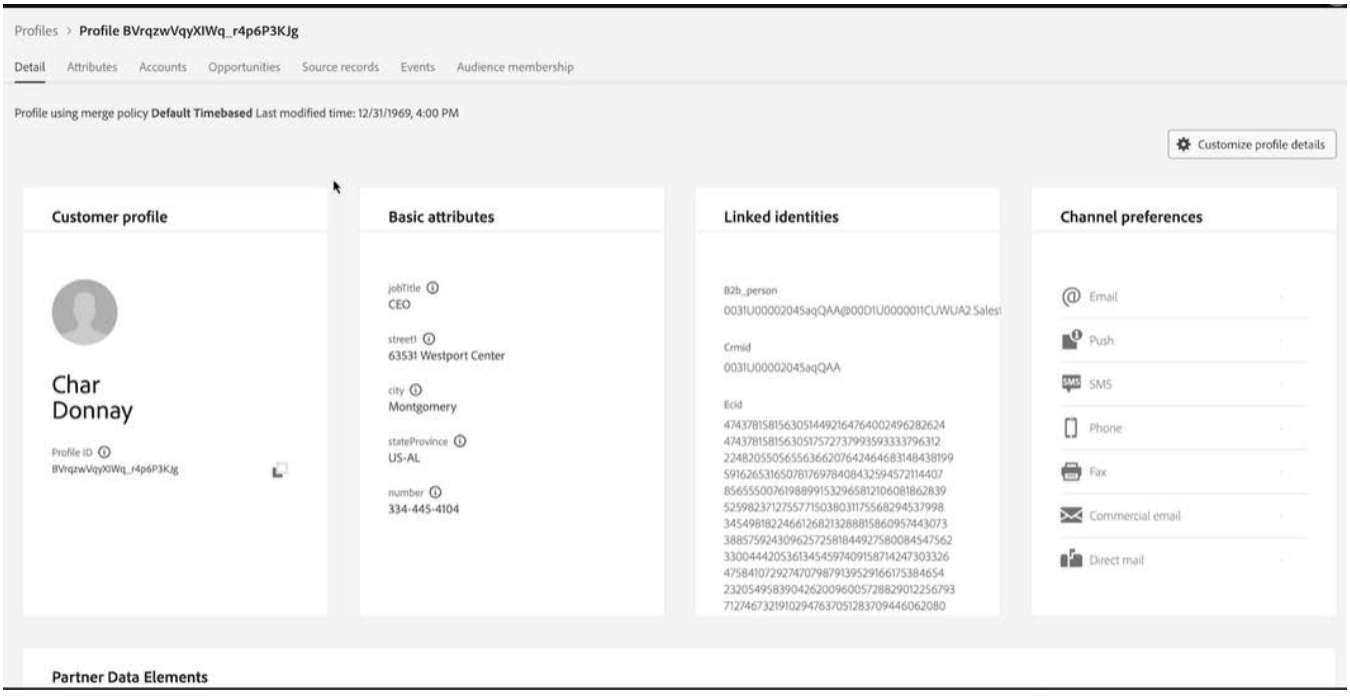
59. The Adobe Real-Time CDP ingests data from multiple sources (e.g., Adobe Analytics, offline data, and other integrated sources), and then uses the Adobe Experience Platform Identity Service to stitch this data into a comprehensive profile, tracking ***both*** identity and user's unique (and private) interactions. **Figure 8** explains how Real-Time Customer Profiles are used with Adobe's other services.

FIGURE 8[6]



60. What this Adobe-Real Time Customer Profile looks like is depicted in **Figure 9**.

FIGURE 9[7]



[6] *Real-Time Customer Profile Guide*, ADOBE, INC., https://experienceleague.adobe.com/en/docs/experience-platform/profile/home (last visited April 2, 2025).

[7] *Create and Enhance Customer Profiles*, ADOBE, INC., https://business.adobe.com/products/real-time-customer-data-platform/create-enhance-customer-profiles.html#marquee (last visited April 2, 2025).

61. As shown in **Figure 9**, Adobe Real-Time CDP includes a dashboard similar to the identity graph (i.e., listing name, Profile ID, address, phone number, and linked identities (like ECID)), but also provides even ***more*** information as indicated by the tabs at the top. This profile includes user's "attributes", "accounts", "opportunities", "source records", "events", and "Audience membership."

62. Using Adobe Real-Time CDP, Adobe aggregates all the user's activities at the account level and attaches them to the user's profile. Adobe Real-Time CDP allows Adobe customers to create audiences directly through this dashboard, which allows filtering based on unique user attributes. For instance, a customer can select a custom age range (35-44), gender (female), and even more specific behavioral information like whether the individuals in the audience are "health conscious." Adobe Real-Time CDP will then search and analyze all other users and find those who fit the audience requirements.

63. Adobe customers can also "enrich" user profiles using Adobe's intelligence services, as well as generate propensity scores (i.e., how likely they are to take a certain action or churn) and create new leads. All this new information is added back to the user profile. Adobe Real-Time CDP thus enabled comprehensive advertising and marketing at the user-level—exactly what current privacy mechanisms are designed to avoid.

REAL-WORLD EXAMPLES

64. Plaintiff Rapak is a Marriott Bonvoy member who frequently visits the Marriott website, which incorporates a host of services encompassed in the Adobe Experience Cloud Platform.

65. Marriott's web properties include the Adobe Experience Platform Launch script. This can be observed through developer tools common on many web browsers, which indicates the script is triggering a request to "assets.adobetm.com." This script enables Adobe products to work together and defines who and when "tags" fire based on the individual's interactions on a page, which are known as events.

66. Separately, Marriott's web properties also incorporate Adobe Analytics, as indicated by the presence of "AppMeasurement.min.js" and Adobe Audience Manager, as confirmed by "Module_AudienceManagement.min.js."

67. Network traffic shows that, when a Marriott user takes action on the Marriott website, such as browsing for hotels, Adobe intercepts (1) ECID; (2) the previously full-string URL the user visited (for

example, showing the user moved from search results to calendar view for hotel prices); (3) the present full-string URL (for instance, indicating the user is viewing the "Rate[]Calendar" for a property with the ID code for the property selected, such as MIATX (i.e., Miami Airport Marriott); and (4) the Company ID (indicating the entity being communicated with is Marriott).

68. This is just one example. Thousands of other websites also incorporate services encompassed within the Adobe Experience Cloud Platform.

69. For instance, when an individual visits Cedars-Sinai's website, this also triggers the Adobe Experience Platform Launch script. Like above, this can be observed through developer tools, which indicates the script is triggering a request to "assets.adobetm.com."

70. If a user navigates to Cedar-Sinai's primary care page and then proceeds to the online scheduling page, this information is intercepted by Adobe based on a review of the network traffic. Adobe receives: (1) ECID; (2) the previous full-string URL the user visited (www.cedars-sinai-org/programs/primary-care.html); (3) the present full-string URL (www.cedars-sinai.org/programs/primary-care/digital-scheduling.html); (4) that the user is engaging in online schedule (as indicated by "hasOnlineScheduling:true"); (5) the Adobe Org ID (indicating the data comes from Cedar Sinai); and (6) the Company ID (relaying the same as Adobe Org ID).

71. This data is sent to Adobe Edge Network, which is used by Adobe's Customer Journey Analytics (CJA), Adobe Real-Time CDP, Adobe Journey Optimizer, and Adobe Target. These destinations suggests that Cedars-Sinai compiles this data in, at least, Adobe Real-Time Customer Profiles (described above). Indeed, Adobe automatically promotes customers using Adobe Experience Platform Edge Network to send and merge the data with Real-Time Customer Profiles.

72. Separately, users who visit Cedars-Sinai trigger "AppMeasurement.min.js" which indicates that Cedars-Sinai is also an Adobe Analytics customer using its traditional integration. This script also enables sending data directly to Adobe Analytics.

PLAINTIFF AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION OF PRIVACY

73. Internet users do not expect to be tracked across every single one of their internet-connected devices, including their web browser, apps, TVs, and more.

74. Indeed, the advent of privacy-preserving mechanisms like Apple's "Do Not Track" feature, which can prevent companies from collecting IDFA/ADID from individuals who opt-out, and similar features described above, have confirmed this expectation.

75. One study by Flurry Analytics in 2021 shows that 88% of iOS users worldwide have availed themselves of this feature, indicating an intent to prevent apps from tracking them on their mobile devices.

76. Users do not know—and did not expect—that Adobe would circumvent these protections by creating a new identifier that is even better than IDFA/ADID at tracking them across services.

77. Adobe itself does not provide any information for Plaintiff and Class Members to understand which websites or online services use ECID or any of Adobe's other privacy-offending products, such that they have no way of uncovering which services do or do not contain Adobe's tracking technology.

78. Plaintiff and Class Members reasonably expect that their online activity would not be tracked by an unknown company, let alone that it would be used to target them across online services for profit.

79. Adobe did not have consent to perform this type of omni-present cross-device tracking using Plaintiff's and Class Members' unique identifiers and private communications.

ADOBE'S CONDUCT VIOLATES ESTABLISHED DATA PRIVACY REGIMES

80. The GDPR and CCPA both mirror Fair Information Practice Principles (FIPPs). Two of the core tenants of FIPPs are (1) clear user consent; and (2) data minimization.

81. Adobe does neither of these things. Despite creating a cross-device persistent user identifier, Adobe makes zero effort to ensure Plaintiff and Class Members are even aware of where this technology is used. This is clear from its own Privacy Policy, which makes no attempt to identify the entities using its services.

82. Separately, the creation of an ever-present persistent identifier is directly at odds with the idea of data minimization, which requires that data should be stored and used only for the period of time in which that data is necessary. Indeed, the fact that device and user-specific identifiers are persistent (and not deleted) is exactly why even device identifiers like IDFA are being phased out by companies like

Apple to preserve users' privacy. Adobe's creation of a maximized identity profile—linking all existing identifiers together—is a regression from today's privacy norms.

TOLLING & CONCEALMENT

83. The earliest Plaintiff and Class Members could have discovered Adobe's conduct was shortly before the filing of this Complaint. Plaintiff became aware of Adobe conduct through communications with counsel that are protected from disclosure.

84. Plaintiff and Class Members, despite their due diligence, could not have discovered Adobe's conduct by virtue of how its technology works and its lack of disclosures.

85. Adobe's interception of unique identifiers, including ECID, and other personal data and other identifiers happens inconspicuously in the background. This process is undetectable to an ordinary person, highly technical, and prevented Plaintiff and any Class Member from uncovering it.

86. Adobe had exclusive knowledge that ECID, its other identifiers, and its tracking technology were tracking Plaintiff and Class Members across the internet alongside their private communications on third-party apps, websites, and other services. Similarly, Adobe had exclusive knowledge that it was using this information to propagate one of the largest targeted advertising systems.

87. Adobe's fraudulent conduct prevented Plaintiff and Class Members from discovering its conduct. Adobe maintained a privacy policy that lacked adequate disclosures for Plaintiff and Class Members to uncover that Adobe even intercepted, had, or used their data. Adobe publicly held out its identifiers and technology as privacy-preserving mechanisms, even though they were not.

88. Adobe was under a duty to disclose the nature and significance of its data interception and use practices—especially in light of its public statements—but did not do so. Adobe is therefore estopped from relying on any statute of limitations by virtue of the discovery rule and doctrine of fraudulent concealment.

CLASS ACTION ALLEGATIONS

89. Plaintiff brings this action under Fed. R. Civ. P. 23 individually and on behalf of the following Classes:

> **Identifier Class:** All natural persons in the United States for whom Adobe intercepted or stored an ECID, demdex cookie, or other identifying information, or for whom Adobe created an Identity Graph.

> **Communications Class:** All natural persons in the United States who had their communications with third parties intercepted or used by Adobe without their consent.

90. The Classes exclude: (1) any judge presiding over this action or their immediate families; (2) Adobe, its subsidiaries, affiliates, parents, successors, predecessors, and any other entity in which Adobe has a controlling interest; (3) Adobe's current and former employees, officers, and directors; and (4) Plaintiff's and Adobe's counsel.

91. ***Numerosity.*** While the precise size of the Classes are currently unknown to Plaintiff, each of the Classes consists of well over a million individuals and members of each of the Classes can be identified through Adobe's records.

92. ***Predominant Common Questions.*** The Classes' claims present several common questions of law and fact that predominant over questions (if any) that affect individual class members. This includes:

a. Whether Adobe violated Plaintiff's and the Classes' privacy rights;

b. Whether Adobe engaged in unfair and deceptive conduct;

c. Whether Adobe's acts and practices violate the California Invasion of Privacy Act;

d. Whether Plaintiff and Class Members are entitled to damages and/or equitable relief, including injunctive relief, restitution, and disgorgement; and

e. Whether Adobe was unjustly enriched.

93. ***Typicality.*** Plaintiff's claims are typical of all Class Members because they arise from the same conduct and are based on the same legal theories.

94. ***Adequate Representation.*** Plaintiff will (and has) fairly and adequately represented the Classes and protected the interest of all Class Members. Plaintiff has retained competent counsel with significant experience in class action and data privacy litigation. Plaintiff and counsel have no interest that conflicts with the interests of the Classes and is not subject to any unique defenses. Plaintiff and their counsel will vigorously prosecute this action to advance the interest of the Classes and have the resources necessary to do so.

95. ***Substantial Benefits.*** A class action is superior to all other possible methods to fairly and efficiently adjudicate this case and controversy, and joinder of all Class Members is impracticable.

Proceeding as a class case has significant advantages to individual litigation, including: (1) comprehensive oversight by a single court, which avoids inconsistent outcomes; and (2) saving time and expense by litigating the same claims arising from the same conduct all in one action.

96. Plaintiff reserves all rights to revise or modify the class allegations based on facts and legal developments following additional investigation or discovery.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

97. California law applies to every Class Member's claims. Adobe maintains its principal place of business in California and conducts substantial business in California, including the activities giving rise to Plaintiff's and Class Members' claims. Adobe's decision to reside in California and avail itself of California's laws makes the application of California law to its conduct alleged herein constitutionally permissible. Adobe also elects to apply California law in its Terms of Use and Privacy Policy.

98. Under California's choice of law rules, the application of California law is appropriate because California has significant contacts to the claims and Parties in this action, California has a greater interest in applying its laws, given Adobe's residency in the State and the location of the conduct at issue, over any other state.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Violation of Common Law Invasion of Privacy (Intrusion Upon Seclusion)
On Behalf of the Plaintiff and Classes

99. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

100. Intrusion upon seclusion requires pleading: (1) that the defendant intruded on a place, conversation, or matter in which Plaintiff has a reasonable expectation of privacy; and (2) that the intrusion would be highly offensive to a reasonable person.

101. Adobe's collection, interception, and use of Plaintiff's and Class Members' personally identifiable information constitutes an intentional intrusion. As does its use of this information to create "identity graphs," the latter of which is based off these identifiers to track and profile Plaintiff and Class Members based on their online activity.

102. Adobe's interception and use of Plaintiff's and Class Members' private online communications, associated with their assigned ECID and other identifying information, is likewise an intentional intrusion upon Plaintiff's and Class Members' solitude.

103. Plaintiff and Class Members reasonably expected their unique identifiers and other personal data, alongside their online activity, would not be intercepted or used by an unknown third-party. The types of identifying information Adobe stored in "identity graphs" are particularly private because they are often directly identifiable, permanent identifiers (e.g., IP address, phone number, email). Plaintiff and Class Members reasonable expected this information would remain private and confidential and would not be intercepted or used by third parties without their consent.

104. This expectation is particularly heightened given that there were no disclosures of Adobe's involvement in intercepting, processing, and using their unique identifiers and other personal data and online communications.

105. Plaintiff and Class Members did not consent to, authorize, or understand Adobe's interception or use of their private data.

106. Adobe's conduct is highly offensive because it violates established social norms. Consumers do not expect to be surveilled whenever they use the internet, especially in light of state laws requiring companies to make adequate disclosures regarding their collection and use of data.

107. Adobe's conduct is particularly offensive in light of the secretive nature in which it takes place. Plaintiff and Class Members had no way of knowing Adobe collected their unique identifiers and other personal data and other online communications, and Adobe did so from thousands of websites, if not more.

108. Adobe's conduct caused Plaintiff and Class Members harm and injury, including a violation of their privacy interests.

109. Plaintiff and Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by Adobe as a result of its intrusion upon seclusion.

110. Defendant's conduct was willful, knowing, and carried out with a conscious disregard for Plaintiff's or Class Members' rights, Plaintiff's and Class Members are entitled to punitive and exemplary damages.

111. Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

SECOND CAUSE OF ACTION

Violation of Article I, Section 1 of the California Constitution (Invasion of Privacy)
On Behalf of the Plaintiff and Classes

112. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

113. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

114. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

115. The right to privacy in California's Constitution creates a right of action against private and government entities.

116. Plaintiff and Class Members have and continue to have a reasonable expectation of privacy in their personal information, identities, and private data, pursuant to Article I, Section I of the California Constitution.

117. The identifiable and private information Adobe intercepted, stored, and used without Plaintiff's and Class Members' consent was used to track them consistently, and persistently, across internet-connected services and to serve targeted advertisements. The manner in which Adobe intercepted this information defeated established privacy-mechanisms and social norms.

118. This conduct constitutes an extremely serious invasion of privacy that would be highly offensive to a reasonable person. Reasonable individuals do not expect that there is an entity intercepting and monitoring all of their online activity, let alone using it for profit.

119. Adobe's conduct violated the privacy of hundreds of thousands (if not millions) of Class Members, including Plaintiff. Adobe did not have consent to intercept this information, let alone use it.

120. Plaintiff and Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by Adobe as a result of its intrusion upon seclusion.

121. Defendant's conduct was willful, knowing, and carried out with a conscious disregard for Plaintiff's or Class Members' rights, Plaintiff and Class Members are entitled to punitive and exemplary damages.

122. Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

THIRD CAUSE OF ACTION
Violation of the California Invasion of Privacy Act ("CIPA")
Cal. Penal Code § 631
On Behalf of the Plaintiff and Classes

123. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

124. CIPA § 631 prohibits any person who by means of any "machine, instrument, contrivance" or in "any other manner:" (1) intentionally taps or makes an unauthorized connection with "any telegraph or telephone wire, line, cable, or instrument;" (2) willfully and without consent of "all parties to the communication" or in "any unauthorized manner" reads or "attempts to read" or "learns the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within" California; (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way" information so obtained; or (4) from aiding, agreeing, employing, or conspiring with "any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

125. Adobe is a person under CIPA § 631.

126. Adobe maintains its principal place of business in California, which is where it designed, created, conspired, and effectuated the interception and use of Plaintiff's and Class Members' unique identifiers and other personal data and private communications.

127. Adobe's technology (e.g., the Adobe Data Collection Tag, Adobe Experience Cloud ID (ECID) framework, etc.), and Plaintiff's and Class Members' computers, mobile devices, and connected TVs, are each a "machine, instrument, contrivance, or . . . other manner" under CIPA § 631.

128. At all relevant times, Adobe used its technology to make unauthorized connections with the lines of communication and instruments used by Plaintiff and Class Members to access online services without the consent of all parties to those communications.

129. Adobe willfully, and without consent, read or attempted to read, or learn the contents and meaning of, Plaintiff's and Class Members' communications with online services while those communications were in transmit or passing over a wire, line, or cable, or were being sent or received within California through its tracking technology, as described herein. This interception happens prior to or at the same time they would be received by the intended recipient.

130. Adobe used, and attempted to use, these identifiable, private communications for its own benefit, including targeted advertising as described herein.

131. Adobe also aided, agreed with, employed, and conspired with website operators and advertising entities to intercept and use this data for profit.

132. The interception and use of Plaintiff's and Class Members' communications was without authorization or consent from Plaintiff and Class Members.

133. Plaintiff and Class Members have been harmed as a result of Adobe's conduct. Their private data has been intercepted, viewed, and used for targeted advertising and has not been destroyed. Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

134. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

FOURTH CAUSE OF ACTION
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 632
On Behalf of the Plaintiff and Classes

135. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

136. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication[.]"

137. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

138. Plaintiff's and Class Members' communications with online services are confidential communications for purposes of § 632 because Plaintiff and Class Members had an objectively reasonable expectation of privacy in this data.

139. Plaintiff and Class Members expected their communications would not be shared with Adobe, as there were no disclosures that Adobe would secretly eavesdrop upon or record their information and communications.

140. Adobe's tracking technology is an electronic amplifying or recording devices for purposes of § 632.

141. By contemporaneously intercepting and recording Plaintiff's and Class Members' confidential and identifiable communications to online services through this technology, Adobe eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

142. At no time did Plaintiff or Class Members consent to Adobe's conduct, nor could they reasonably expect that their communications with online services would be overheard and recorded by Adobe.

143. Adobe utilizes these private communications for their own benefit, including to serve targeted advertisements and develop user profiles.

144. Plaintiff and Class Members have been harmed as a result of Adobe's conduct. Their private data has been intercepted, viewed, and used for targeted advertising and has not been destroyed.

Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

145. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

FIFTH CAUSE OF ACTION
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 638.50 & 638.51
On Behalf of the Plaintiff and Classes

146. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

147. CIPA § 638.50(b) defines a "pen register" as a "device or process" that "records or decodes dialing, routing, addressing, or signaling information" that is "transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

148. Separately, CIPA § 638.50(c) defines a "[t]rap and trace device" as a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication."

149. CIPA § 638.51 prohibits a person from installing either a pen register or trap and trace device without a court order.

150. Adobe is a person under CIPA § 638.51.

151. Adobe implemented and installed the ECID framework—which are pen registers and/or trap and trace devices—on Plaintiff's and Class Members' devices and browsers.

152. These processes captured "routing, addressing, or signaling information" because they intercept: (1) unique user and device identifiers; and (2) the Adobe Org ID (indicating the website to whom the user is communicating).

153. Adobe was not authorized by any court order to use a pen register or trap and trace device to record or capture Plaintiff's and Class Members' routing, addressing, or signaling information.

154. Plaintiff and Class Members did not consent to Adobe's installation of a pen register or trap and trace device on their devices and browsers.

155. Plaintiff and Class Members have been harmed as a result of Adobe's conduct. Adobe did not have authorization to use pen registers and/or trap and trace devices to surveille and identify Plaintiff and Class Members or other routing, addressing, and signaling information revealing who the intended recipients of their communications were.

156. Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

157. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

SIXTH CAUSE OF ACTION
Violation of the Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502 ("CDAFA")
On Behalf of the Plaintiff and Classes

158. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

159. The California Legislature enacted CDAFA to "expand the degree of protection afforded. . . from tampering, interference, damage, and unauthorized access to ([including the extraction of data from)] lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals . . ." Cal. Penal Code § 502(a).

160. Plaintiff's and Class Members' devices on which Adobe's tracking technology is installed, including their computers, smart phones, and tablets, constitute "Computer system" within the meaning of the CDAFA. *Id.* § 502(b)(5).

161. The data that Adobe accessed and collected from Plaintiff's and Class Members' devices constitute "Data" within the meaning of the CDAFA. *Id*. § 502(b)(8).

162. Defendant Adobe violated § 502(c)(1) of the CDAFA by knowingly accessing without permission Plaintiff's and Class Members' devices in order to wrongfully obtain and use their personal data, in violation of users' reasonable expectations of privacy in their devices and data.

163. Defendant Adobe violated § 502(c)(2) of the CDAFA by knowingly and without permission taking, copying, and making use of Plaintiff's and the Class Members' unique identifiers and other personal data from their devices.

164. Defendant Adobe's tracking technology incorporated on Plaintiff's and the Class Members' devices constitute "computer services" within the meaning of the CDAFA. Defendant Adobe violated § 502(c)(3) by knowingly and without permission using those computer services, and/or causing them to be used. Defendant Adobe violated § 502(c)(7) by knowingly and without permission accessing those devices, and/or causing them to be accessed.

165. Defendant Adobe violated §§ 502(c)(6) and (c)(13) of the CDAFA by knowingly, and without permission from Plaintiff and the Class Members, providing and/or assisting in providing advertisers and website owners the ability to access Plaintiff's and the Class Members' personal data via its Tracking Technology.

166. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information." Defendants Adobe violated § 502(c)(8) by knowingly and without permission introducing a computer contaminant via its tracking technology incorporated on Plaintiff's and the Class Members' devices, which intercepted their personal data. As described *supra*, the tracking technology is deeply hidden; Plaintiff and Class Members had no way to remove it or opt out of its functionality.

167. Plaintiff and Class Members suffered damage and loss as a result of Adobe's conduct. Adobe's practices have deprived Plaintiff and the Class Members of control over their valuable property (namely, their sensitive personal data), the ability to receive compensation for that data, and the ability to withhold their data for sale.

168. Plaintiff and the Class Members seek compensatory damages in accordance with CDAFA § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

169. Plaintiff and Class Members have also suffered irreparable and incalculable harm and injuries from Adobe's violations. The harm will continue unless Adobe is enjoined from further violations of this section. Plaintiff and Class Members have no adequate remedy at law.

170. Plaintiff and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Adobe's violations were willful and, upon information and belief, Adobe is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294. Plaintiff and the Class Members are also entitled to recover their reasonable attorneys' fees under § 502(e)(2).

SEVENTH CAUSE OF ACTION
Unjust Enrichment
On Behalf of the Plaintiff and Classes

171. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

172. Adobe receives benefits from Plaintiff and Class Members in the form of their unique identifiers and other personal data and private online communications. Adobe acquired this information without Plaintiff's and Class Members' authorization and without providing corresponding compensation.

173. Adobe acquired and used this private data for its own benefit, including tangible economic benefits from companies that used Adobe for targeted advertising.

174. Had Plaintiff and Class Members known of Adobe's misconduct, they would not have agreed Adobe could acquire and use their private data.

175. Adobe unjustly retained these benefits at the expense of Plaintiff and Class Members. Plaintiff and Class Members were harmed by this conduct and were not provided any commensurate compensation.

176. The benefits Adobe received and derived from Plaintiff and Class Members' private data rightly belong to Plaintiff and Class Members. It is inequitable under unjust enrichment principles for Adobe to retain the profits and other intangible benefits they derived through its wrongful conduct.

177. Adobe should be compelled to disgorge these profits and other inequitable proceeds in a common fund for the benefit of Plaintiff and Class Members.

EIGHTH CAUSE OF ACTION
Injunctive Relief
On Behalf of the Plaintiff and Classes

178. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

179. Adobe's conduct has and continues to cause harm to Plaintiff and Class Members' privacy and autonomy, as it continues to store unique persistent identifiers, as well as the private contents of their communications, on its own systems. Adobe routinely uses this information for targeted advertising.

180. Accordingly, Plaintiff and Class Members seek injunctive relief, including an order permanently restraining Adobe from continuing to use and store this information without consent and/or a court order, and requiring Adobe to delete this information from its systems.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the putative Classes requests the Court enter an Order:

a. Certifying the Classes and appointing Plaintiff as Class Representative;

b. Finding Adobe's conduct unlawful;

c. Awarding injunctive and other equitable relief as is just and proper;

d. Awarding Plaintiff and the Classes statutory, actual, compensatory, punitive, nominal, and other damages, as well as restitution and/or disgorgement of unjust and unlawful profits;

e. Awarding pre-judgment and post-judgment interest;

f. Awarding reasonable attorneys' fees, costs, and expenses; and

g. Granting any other relied as the Court sees just and proper.

JURY DEMAND

Plaintiff demands a trial by jury.

Dated: April 2, 2025

/s/ Willem F. Jonckheer
Robert C. Schubert S.B.N. 62684
Willem F. Jonckheer S.B.N. 178748
Amber L. Schubert S.B.N. 278696
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel.: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
wjonckheer@sjk.law
aschubert@sjk.law

Christian Levis (*pro hac vice* forthcoming)
Amanda Fiorilla (*pro hac vice* forthcoming)
Rachel Kesten (*pro hac vice* forthcoming)
Yuanchen Lu (pro hac vice forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com
ylu@lowey.com

Attorneys for Plaintiff and the Proposed Class